AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

Metodología JARUS
Safety Dependency Analysis

Alberto Gaspar Martín
División UAS

Evento *“Hacia la Automatización de UAS”*
23 Abril 2025

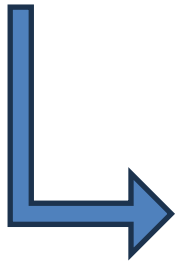
Contenido

- JARUS Methodology
- Anexo B
  - Clasificación de funciones
  - Nivel de automatización
  - Impacto en la seguridad
  - Robustez
  - OSO #XII de SORA v2.5 (old)
  - Use Case I

Metodología JARUS

SORA

Intervención humana = Mitigación
+
Automatización creciente



Joint Authorities for Rulemaking of Unmanned Systems

Joint Authorities for Rulemaking of Unmanned Systems

JARUS Methodology for Evaluation of Automation for UAS Operations

DOCUMENT IDENTIFIER : JARUS-Doc-AutoMethod.1.0

Edition Number	:	1.0
Edition Date	:	April 21, 2023
Status	:	Published
Intended for	:	General Public
Category	:	Publication
WG	:	Automation

Los UAS son sistemas que realizan diversas funciones de forma simultánea. Estas funciones se realizan:

- Por seguridad (Safety oriented)

Funciones necesarias para que el vuelo sea seguro
(Aseguramiento de la envolvente de vuelo, evasión de obstáculos, aseguramiento de la posición…)

- Por motivos operacionales (Operational oriented)

Funciones para realizar la actividad por la que se está volando
(Fotos, vídeo, topografía…)

- Funciones independientes de la seguridad: estas funciones pueden cumplirse en su totalidad por otros medios en caso de que se detecte un fallo o una operación incorrecta.

Redundant

Function not degraded

- Funciones parcialmente dependientes de la seguridad: la funcionalidad se reduciría o degradaría en caso de que se detectara un error o un funcionamiento incorrecto. Este grado de independencia requiere que otros sistemas estén presentes para respaldar.

Redundant

Function degraded

- Funciones dependientes de la seguridad: la función no se puede llevar a cabo por ningún otro medio en caso de falla u operación incorrecta, y el fallo u operación incorrecta de la función resulta en un impacto directo en la seguridad en el área operativa.

Non redundant

Function degraded

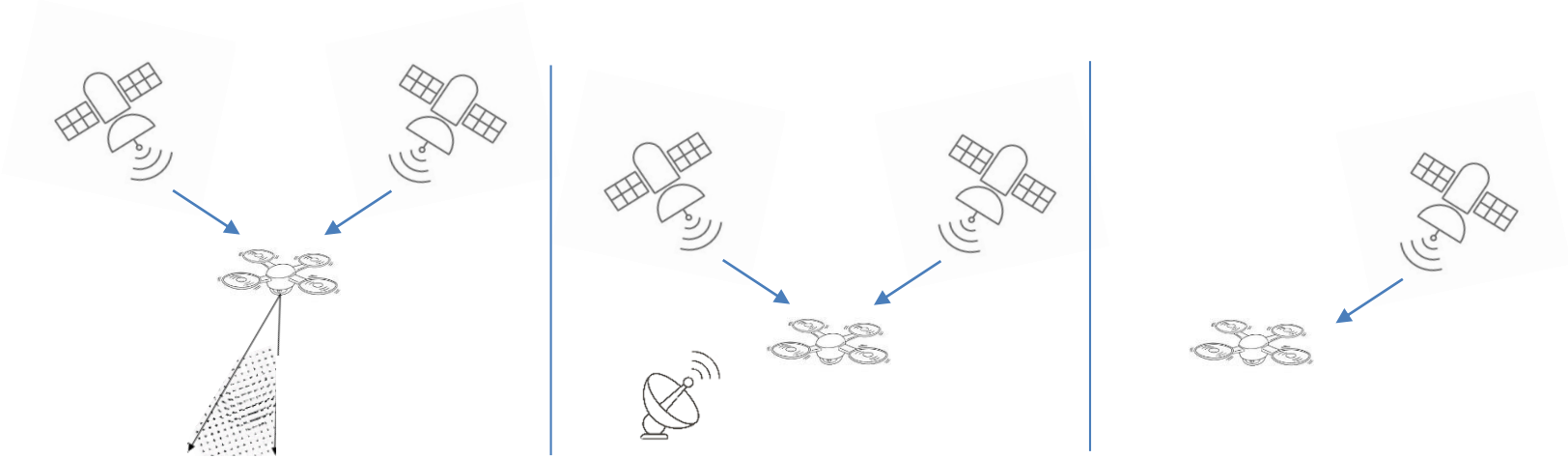
Metodología JARUS

La seguridad de una función depende de dos parámetros:

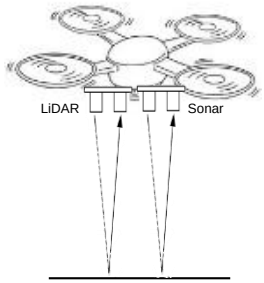
- **Redundancia**: Hay más de dos sistemas realizando la misma función?
- **Limitación operacional:** En caso de un fallo simple del sistema, la función se ve degradada?

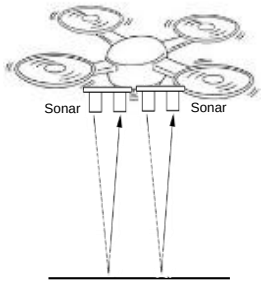
		Redundancia	
		Sí	No
Limitación operacional	Sí	Partially safety dependent	Safety dependent
	No	Safety independent	Operational oriented

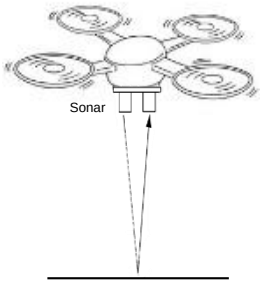
Funciones (Capabilities)	Safety independent	Partially safety dependent	Safety dependent
	Redundante = Sí, Limitación = No	**Redundante = Sí, Limitación = Sí**	**Redundante = No, Limitación = Sí**
Position Assurance	GPS + GALILEO + Posicionamiento por visión	GALILEO + GPS	GPS



Funciones (Capabilities)	Safety independent	Partially safety dependent	Safety dependent
	Redundante = Sí, Limitación = No	**Redundante = Sí, Limitación = Sí**	**Redundante = No, Limitación = Sí**
Terrain and Obstacle Avoidance	LiDAR + Sonar	Doble Sonar	Sonar





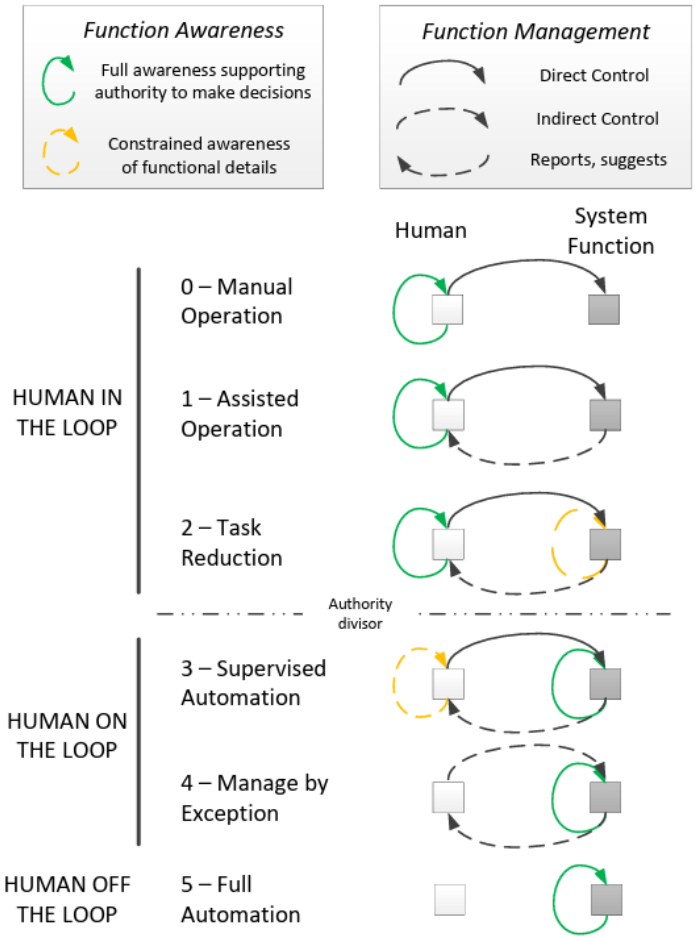


En función de la tecnología utilizada, se diferencian los siguientes casos:

	Tecnología dependiente de factores externos	Tecnología autocontenida
Safety dependent (Redundancia=No, Limitación = Sí)	Un sistema	Un sistema
Partially Safety dependent (Redundancia=Sí, Limitación = Sí)	Dos sistemas (misma o diferente tecnología)	Dos sistemas de la misma tecnología
Safety Independent (Redundancia=Sí, Limitación = No)	Dos sistemas (misma o diferente tecnología) + uno con tecnología autocontenida	Dos sistemas de diferente tecnología

Tecnología dependiente de factores externos: El fallo puede ocurrir por causas externas al sistema integrado en el UAS. (Por ejemplo, la constelación GPS puede fallar independientemente del receptor integrado en el UAS)

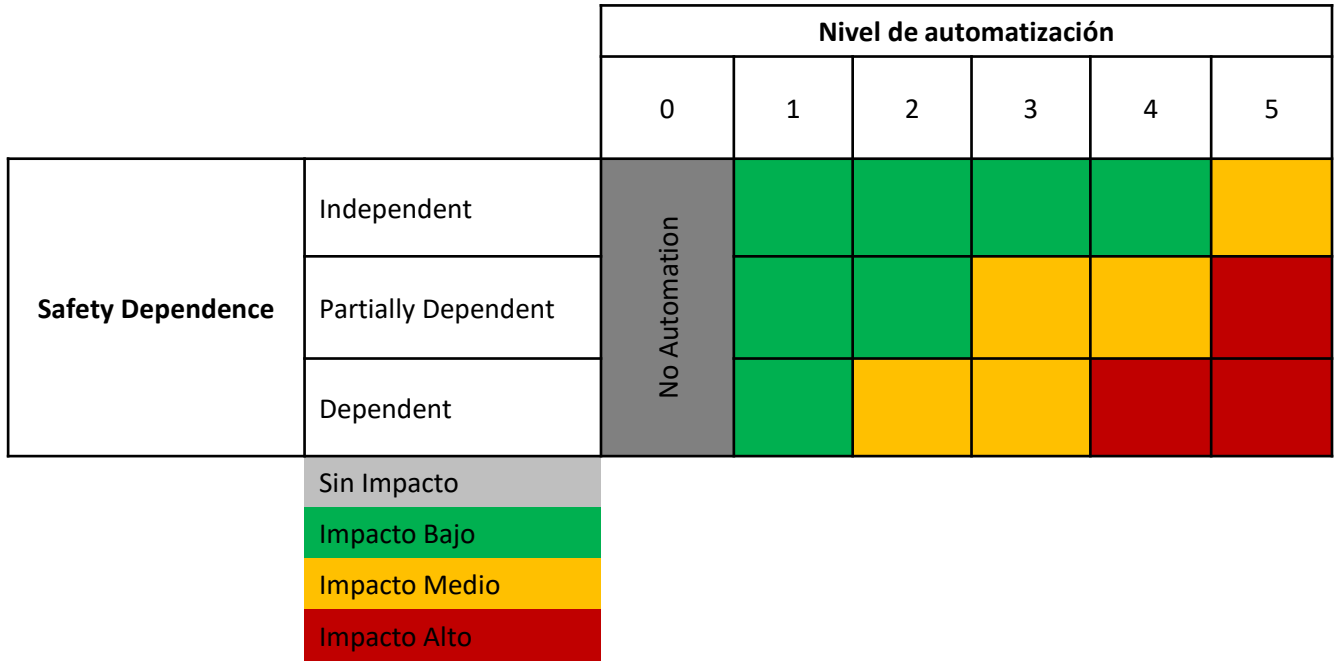
Tecnología autocontenida: Los únicos fallos posibles provienen del propio sistema integrado en el UAS. (Por ejemplo, un anemómetro no puede fallar "por el aire")



	Authority		
Level of Automation	*Normal*	*Abnormal*	*Emergency*
Level 0	Human		
Level 1	Human *AND* Machine[1]	Human	Human
Level 2	Human *AND* Machine		Human
Level 3	Machine	Human *AND* Machine[2]	Human[3, 5]
Level 4	Machine		Human *AND* Machine[4, 5]
Level 5	Machine[5]		

UAS Automation Levels in Flight Operations							
Level / Functions	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Components of Trusted Autonomy**
	Manual Operation	**Assisted Operation**	**Task Reduction**	**Supervised Automation**	**High Automation**	**Full Autonomy**	
Human-Machine Teaming	Human led	Human-In-the-loop	Human-In-the-loop	Human-In/On-the-loop	Human-On-the-loop	Human-Off-the-loop	Human-Machine Symbiosis
Sustained Aircraft Maneuver Control	Human	Human *AND* Machine	Machine (Managed by Human)	Machine (Supervised by Human)	Machine	Machine	Machine
Object and Event Detection and Response (OEDR)	Human	Human	Machine (Managed by Human)	Machine (Supervised by Human)	Machine	Machine	Machine
Fallback (Integrity Thresholds Exceeded)	Human	Human	Human	Human	Fall back Ready Human	Machine (Limited or Segregated Operations)	Optimized Human AND/OR Machine
Communication with External Systems (Ground and Airspace systems)	Human	Human	Human *OR* Machine (Managed by Human)	Machine (Supervised by Human)	Machine	Machine	Machine

Impacto: Importancia de una función para la operación.



La robustez es el nivel de confianza requerido

		Robustez					
SAIL		I	II	III	IV	V	VI
Impacto	Bajo	Bajo	Bajo	Bajo	Bajo	Medio	Alto
	Medio	Bajo	Bajo	Medio	Medio	Alto	Alto
	Alto	Bajo	Medio	Medio	Alto	Alto	Alto

¿Cómo se alcanza el correspondiente nivel de robustez?

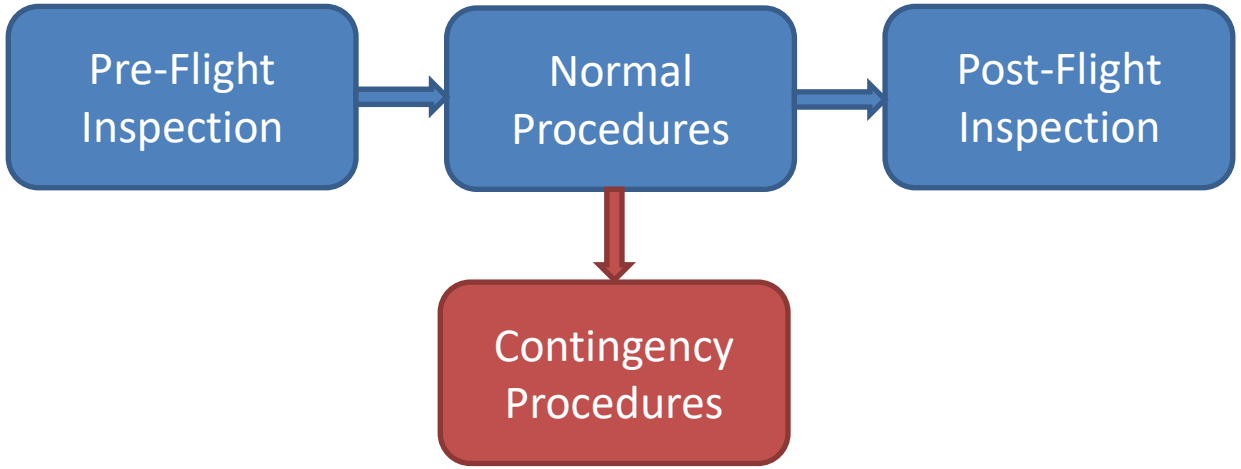
TECHNICAL ISSUE WITH THE UAS		LEVEL of INTEGRITY		
		Low	Medium	High
OSO #XII UAS components essential to safe operations are designed to an Airworthiness Design Standard (ADS)	Criterion	The UAS components essential to safe operations are designed to an Airworthiness Design Standard (ADS)[1] considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority to contribute to the overall safety objective of 10-4/FH for the loss of control of the operation.	The UAS components essential to safe operations are designed to an Airworthiness Design Standard (ADS)[1] considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority to contribute to the overall safety objective of 10-5/FH for the loss of control of the operation.	The UAS components essential to safe operations are designed to an Airworthiness Design Standard (ADS)[1] considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority to contribute to the overall safety objective of 10-6/FH for the loss of control of the operation.
	Comments	[1] *Example of Airworthiness Design Standards (ADS) are:* • *the EASA Special Condition Light-UAS, or* • *the JARUS Certification Specification for Light Unmanned Rotorcraft Systems (LURS), or* • *the JARUS Certification Specification for Light Unmanned Aeroplane Systems (LUAS).*		

	Alternative criterion taking credit for functional test-based methods	A Functional Test-Based (FTB) design appraisal gained by a UAS designer is available and meets the conditions described in section 3(c)(ii), in particular: • 30,000 hours in order to achieve a 95% confidence (assuming a binomial/Poisson distribution for the operational level hazard rate and no failures during the test). • The functional tests supporting the FTB design appraisal gained by a UAS designer have been executed: ○ within the full scope/envelope intended by the UAS Operator. ○ following the maintenance and operational procedures and the remote crew training referred to in the operational authorization.	N/A[2] • The minimum number of test cycles are proportionate to the risk of the operation, with at least: ○ 30 hours for SAIL I; ○ 300 hours for SAIL II; ○ 3,000 hours for SAIL III; and ○ 30,000 hours for SAIL IV in order to achieve a 95% confidence (assuming a binomial/Poisson distribution for the operational level hazard rate and no failures during the test)[3].
	Comments	*N/A*	*[2] Functional test-based method are not considered feasible for operations with a SAIL V or VI*

TECHNICAL ISSUE WITH THE UAS		LEVEL of ASSURANCE		
		Low	Medium	High
OSO #XII UAS components essential to safe operations are designed to an Airworthiness Design Standard	Criterion	The applicant declares that the required level of integrity has been achieved[1].	The applicant has supporting evidence that the required level of integrity is achieved. This is typically done by testing, analysis, simulation[2], inspection, design review or through operational experience.	A competent third party validates the claimed level of integrity.
	Alternative criterion taking credit for functional test-based methods	The Operator declares[3] that the FTB design appraisal gained by a UAS designer have been executed according to principles/standards[2] considered adequate by the competent authority in charge of granting the Operational Authorization.	N/A[4]	

Inspección de línea eléctrica

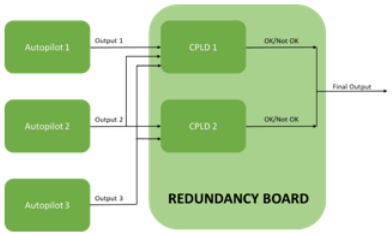
- Casi todas las funciones automatizadas en nivel 5



Inspección de línea eléctrica

- Casi todas las funciones automatizadas en nivel 5

Triple redundancy autopilot



AI Path definition

On Board computer

Optical flow stabilization

Telemetry

Meteorological evaluation

Navigation Aids

Altimeter (Lightware SF11/C)

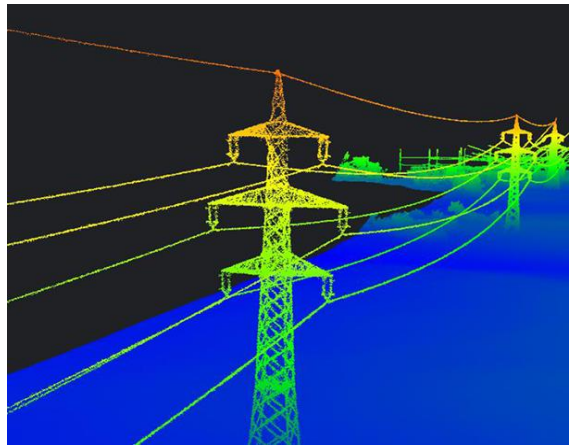
DAA (Casia X + LiDAR)

Payload

Camera

LiDAR mapper

Triple redundancy GNSS receiver



Other systems

Dynamic geocaging (GNSS)

Remote ID

FTS

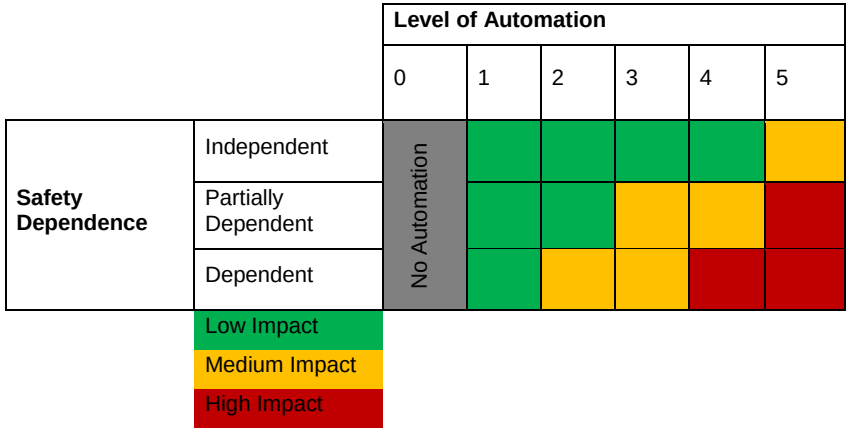
Self-extinguishing system

Annex B - Capabilities

Capability	Redundancy	Limitation	Equipment depending on external factors	Equipment with technology self-contained	Safety Dependence
Position Assurance	Yes	No	3 GNSS	Optical Flow + LiDAR altimeter	Safety Independent
Common Navigation Reference	Yes	No	3 GNSS	Optical Flow + LiDAR altimeter	Safety Independent
Flight Management and Operational Envelope Assurance	Yes	No	-	3 autopilots + 2 CPLD in redundancy board	Safety Independent
Dynamic Systems Coordination	-	-	-	-	-
Multiple System Management	-	-	-	-	-
Tolerable Latencies	-	-	-	-	-
Aircraft Control Handoff	Yes	No	-	3 autopilots + 2 CPLD in redundancy board	Safety Independent
System Status Awareness	-	-	-	-	-
Failure Identification and Annunciation	No	Yes	Failure management integrated in each sensor	Failure management integrated in each sensor	Safety Dependent
Contingency Management	No	Yes	Autopilot with data from each sensor	Autopilot with data from each sensor	Safety Dependent
Safe Landing	Yes	No	3 GNSS	Optical Flow + LiDAR altimeter	Safety Independent
Geographic Limit and Airspace Awareness	Yes	Yes	3 GNSS	-	Partially Safety Dependent
Terrain and Obstacle Avoidance	Yes	Yes	-	LiDAR DAA	Partially Safety Dependent
Aircraft and Airborne Hazard Avoidance	Yes	No	-	LiDAR DAA + Casia C	Safety Independent
Air Traffic Services Communications and Control Guidance	-	-	-	-	-
Sharing Intentions and Contingencies with other Airspace Users	-	-	-	-	-
Weather	No	Yes	WeatherStack	-	Safety Dependent

Annex B - Capabilities

Capability	LoA	Safety Dependence	Impact
Position Assurance	5	Safety Independent	Medium
Common Navigation Reference	5	Safety Independent	Medium
Flight Management and Operational Envelope Assurance	5	Safety Independent	Medium
Dynamic Systems Coordination	-	-	-
Multiple System Management	-	-	-
Tolerable Latencies	-	-	-
Aircraft Control Handoff	5	Safety Independent	Medium
System Status Awareness	-	-	-
Failure Identification and Annunciation	4	Safety Dependent	High
Contingency Management	4	Safety Dependent	High
Safe Landing	5	Safety Independent	Medium
Geographic Limit and Airspace Awareness	5	Partially Safety Dependent	High
Terrain and Obstacle Avoidance	5	Partially Safety Dependent	High
Aircraft and Airborne Hazard Avoidance	5	Safety Independent	Medium
Air Traffic Services Communications and Control Guidance	-	-	-
Sharing Intentions and Contingencies with other Airspace Users	-	-	-
Weather	5	Safety Dependent	High



Annex B - Capabilities

Medium Impact	High Impact	N/A
Position Assurance	Geographic Limit and Airspace Awareness	Dynamic Systems Coordination
Common Navigation Reference	Terrain and Obstacle Avoidance	Multiple System Management
Flight Management and Operational Envelope Assurance	Weather	Tolerable Latencies
Aircraft Control Handoff	Failure Identification and Annunciation	System Status Awareness
Safe Landing	Contingency Management	Air Traffic Services Communications and Control Guidance
Aircraft and Airborne Hazard Avoidance		Sharing Intentions and Contingencies with other Airspace Users

Annex B

		Robustness					
SAIL		I	II	III	IV	V	VI
Impact	Low	Low	Low	Low	Low	Medium	High
	Medium	Low	Low	Medium	Medium	High	High
	High	Low	Medium	Medium	High	High	High

Capability	Impact	SAIL	Robustness
Position Assurance	Medium	II	Low
Common Navigation Reference	Medium	II	Low
Flight Management and Operational Envelope Assurance	Medium	II	Low
Dynamic Systems Coordination	-	II	-
Multiple System Management	-	II	-
Tolerable Latencies	-	II	-
Aircraft Control Handoff	Medium	II	Low
System Status Awareness	-	II	-
Failure Identification and Annunciation	High	II	Medium
Contingency Management	High	II	Medium
Safe Landing	Medium	II	Low
Geographic Limit and Airspace Awareness	High	II	Medium
Terrain and Obstacle Avoidance	High	II	Medium
Aircraft and Airborne Hazard Avoidance	Medium	II	Low
Air Traffic Services Communications and Control Guidance	-	II	-
Sharing Intentions and Contingencies with other Airspace Users	-	II	-
Weather	High	II	Medium

Annex B

Low Robustness	Medium Robustness	N/A
Position Assurance	Geographic Limit and Airspace Awareness	Dynamic Systems Coordination
Common Navigation Reference	Terrain and Obstacle Avoidance	Multiple System Management
Flight Management and Operational Envelope Assurance	Weather	Tolerable Latencies
Aircraft Control Handoff	Failure Identification and Annunciation	System Status Awareness
Safe Landing	Contingency Management	Air Traffic Services Communications and Control Guidance
Aircraft and Airborne Hazard Avoidance		Sharing Intentions and Contingencies with other Airspace Users

Declaración de 300 horas de FTB

Evidencias de 300 horas de FTB

Muchas gracias

Web AESA UAS/Drones